

# Current Cybersecurity trends & Responses in Korea

Yong Seok Oh, Manager  
CISSP, ISMS

Korea Internet & Security Agency  
October 2015

# Contents

---

I ✓ Cyber Security Incidents

II ✓ Cyber Security Policy & Strategy

III ✓ Recent Cyber Security Strategies

IV ✓ GCCD & CAMP

# I Cyber Security Incidents

---

# Major Incidents in Korea

2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014

1

2

3

4

5

6

7

8

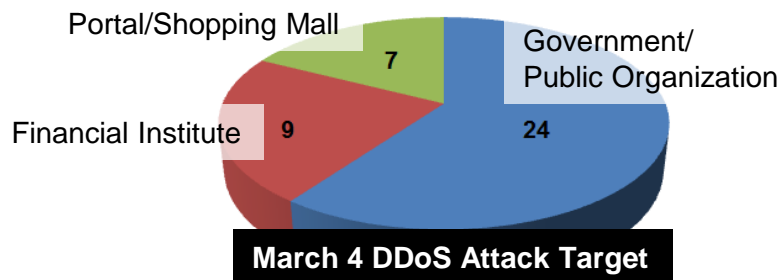
9

No.	Date	Cyber Attack
1	2003. 1	A computer virus shut down servers at the country's largest Internet service provider, KT Corp, disconnecting five million customers from the web
2	2005. 6	224,400 cases of ID theft were identified by NCSoft (online game company)
3	2008. 2	10,810,000 cases of ID theft were identified by Auction Korea (online shopping company)
4	2009. 7	7.7 DDoS attack to portal sites, online bank and government's homepages in US and South Korea occurred
5	2011. 9	35,000,000 cases of ID theft were identified by SK Communications (portal site)
6	2013. 3	Major television broadcasters and banks were under cyber attack (48,700 PCs, Servers and ATMs were damaged)
7	2013. 6	The websites of S. Korea's presidential office, government agencies and some media organizations were attacked
8	2014. 1	85 million personal information from KB Card, NH Card, Lotte Card has been disclosed
9	2014. 3	9.8 million personal information from KT has been disclosed

# March 4<sup>th</sup> 2011 DDoS Attack

## □ March 4th DDoS attack in 2011, evolved from July 7th DDoS in 2009

**Overview – DDoS attack** targeting 40 major Korean websites



Classification	Mar 4	Jul 7
# of Zombie PCs	116,299	115,044
target websites	40	36
# of Blocked C&C servers	748	538
# of destroyed HDDs	756	1,466

March and July DDoS attacks are similar in used no. of exploited zombie PCs and infection method however **March DDoS attack Method is more Intelligent and destructive than July DDoS**

## Implications

Dog and cat fight between KISA and Hacker

KISA Response
Vaccine distribution via <a href="http://www.boho.or.kr">www.boho.or.kr</a>
Effective defense against DDoS Attack
Hard disk damage prevention guideline



Change in Attack Method
Block zombie PC's access to <a href="http://www.boho.or.kr">www.boho.or.kr</a>
Destroy HDD just after the infection
HDD is destroyed even at safe mode booting



# March 20<sup>th</sup> 2013 Cyber Attack

- **Attack on 6 broadcasting and financial companies which destroyed 48,700 PC, Server, ATM**

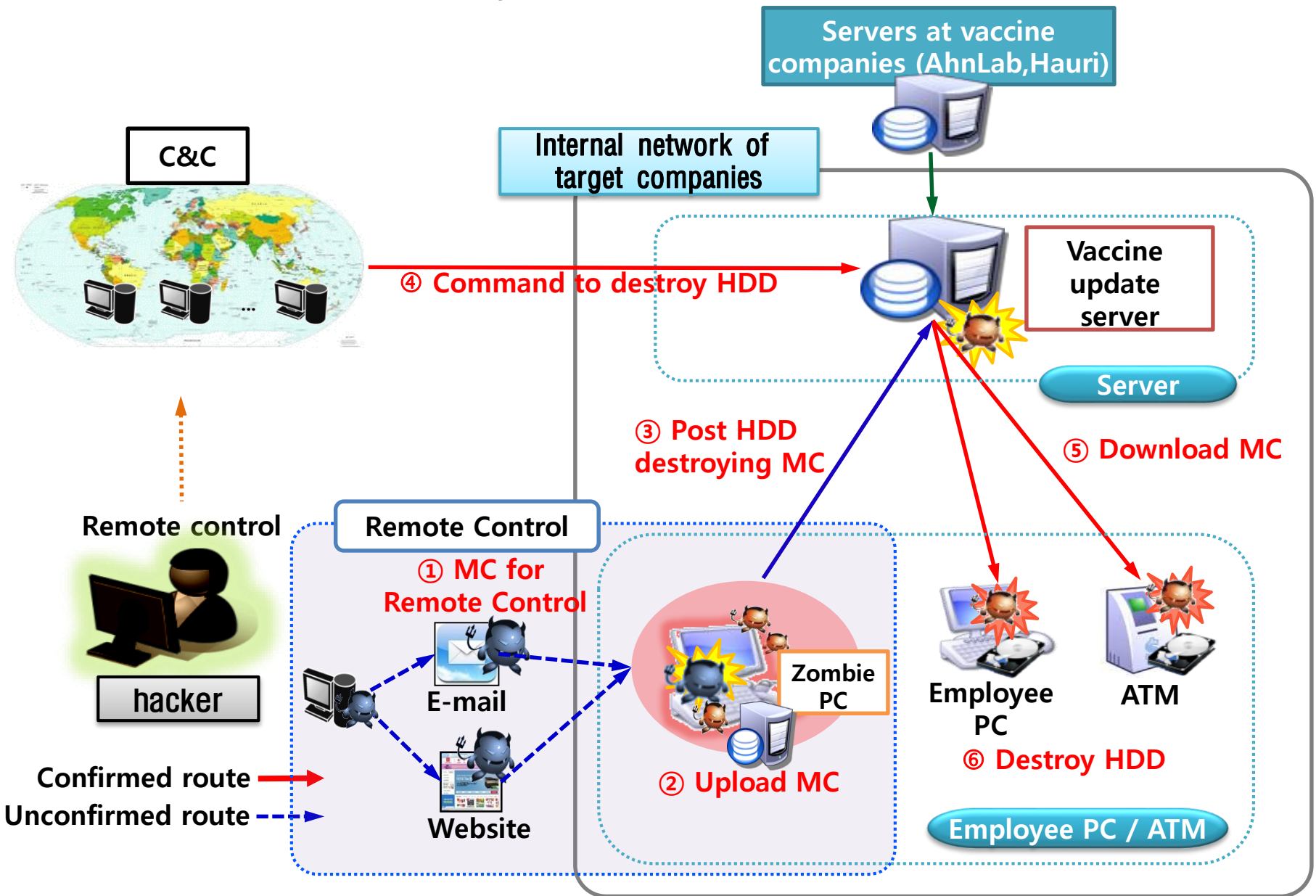
- Distributed MC through “Weather.com” and infected 800 PCs (March 25th)
- Destroyed 58 Digital YTN website servers (March 26th)
- Deleted data from 14 conservative groups’ website (March 26th)

- **Recovered to normal operation (March 29th)**

- Recovery of 58 Digital YTN web servers (April 12th)



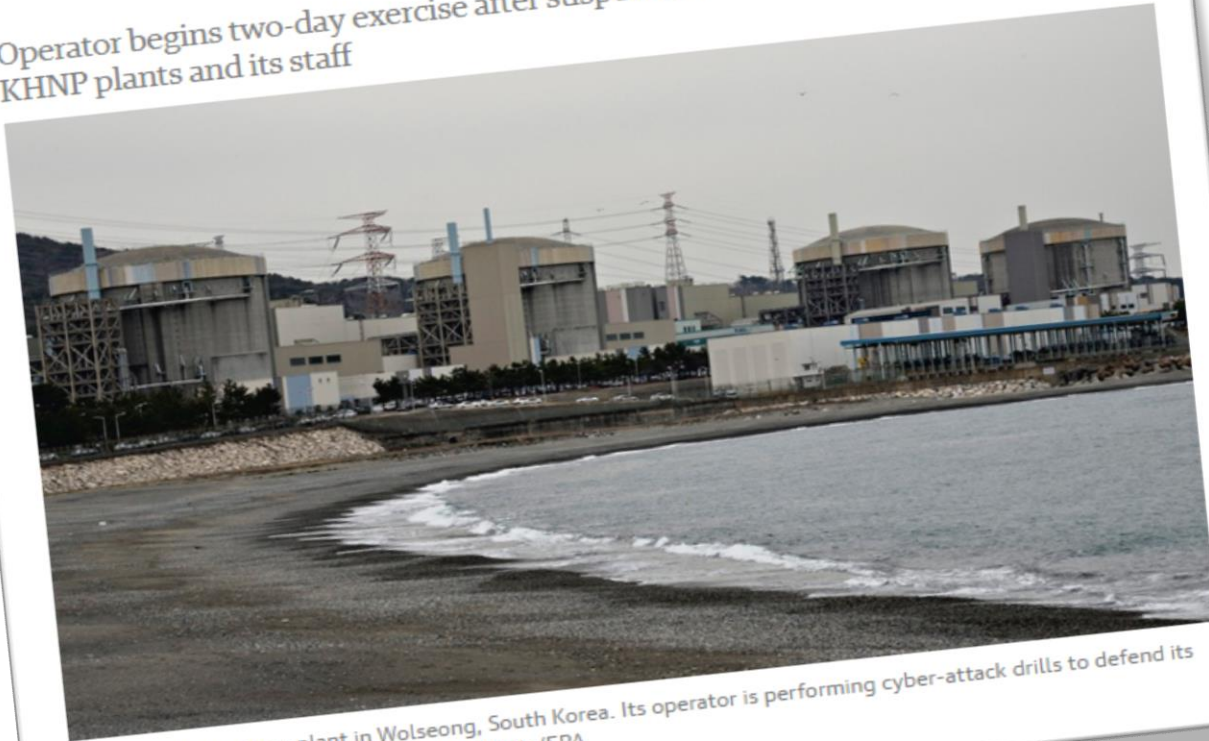
# March 20<sup>th</sup> 2013 Cyber Attack



# Recent Incidents in Korea

## South Korean nuclear operator hacked amid cyber-attack fears

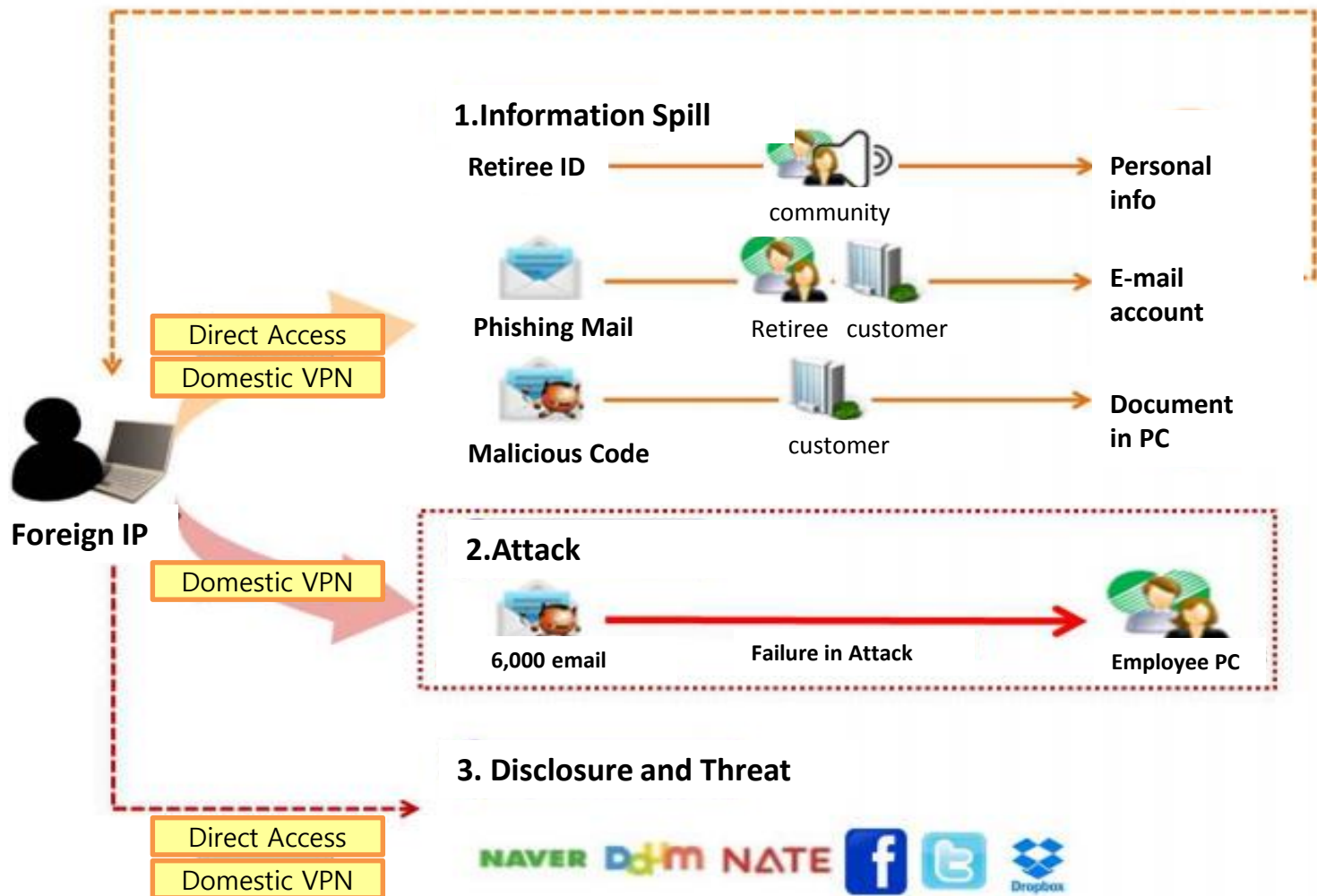
Operator begins two-day exercise after suspected hacker tweets information on KHNP plants and its staff



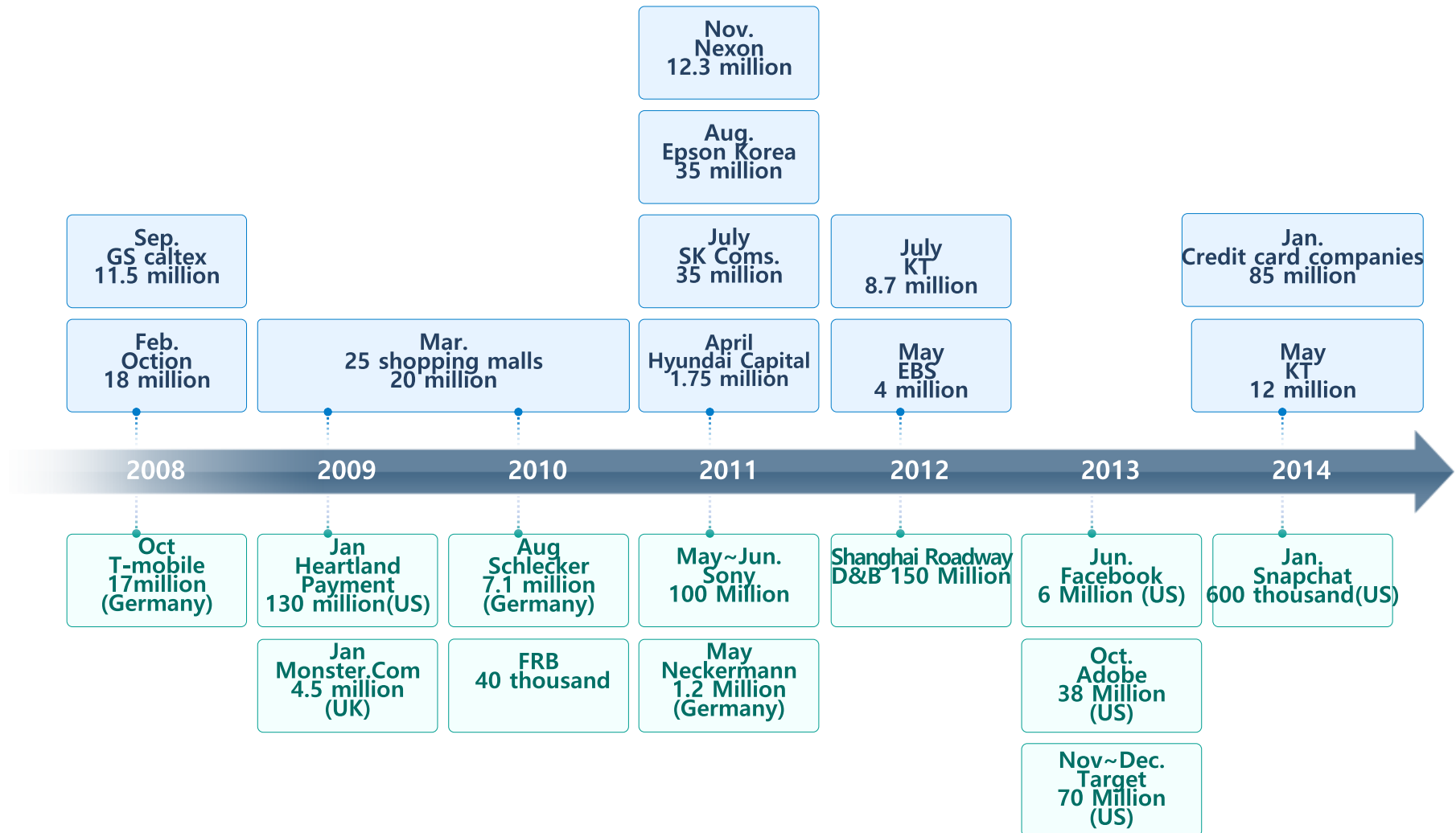
📷 The nuclear power plant in Wolsong, South Korea. Its operator is performing cyber-attack drills to defend its plants against hackers. Photograph: Udo Weitz/EPA

# Recent Incidents in Korea

- Attack Flow to Nuclear operator



# Major Personal Information Infringements Incidents

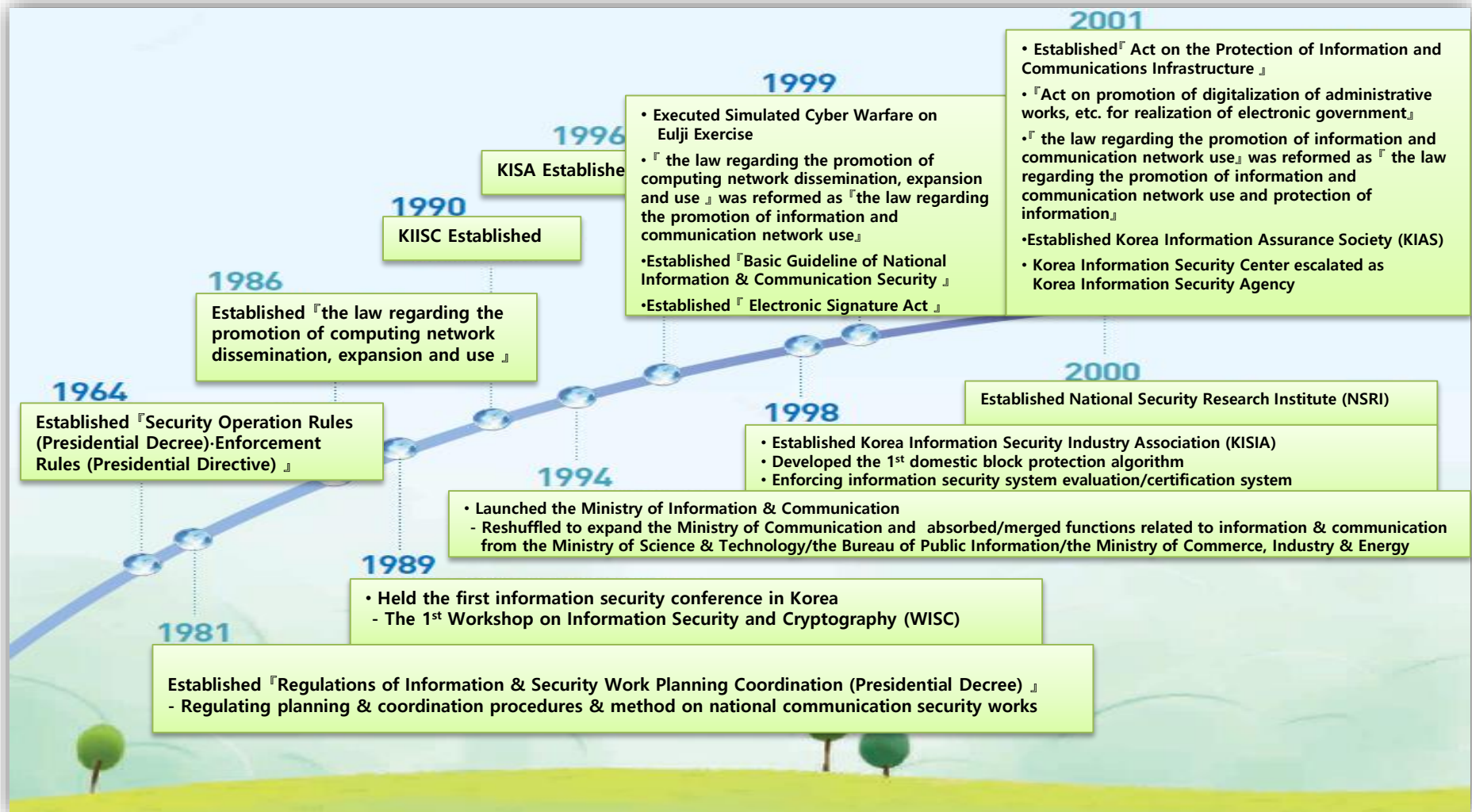




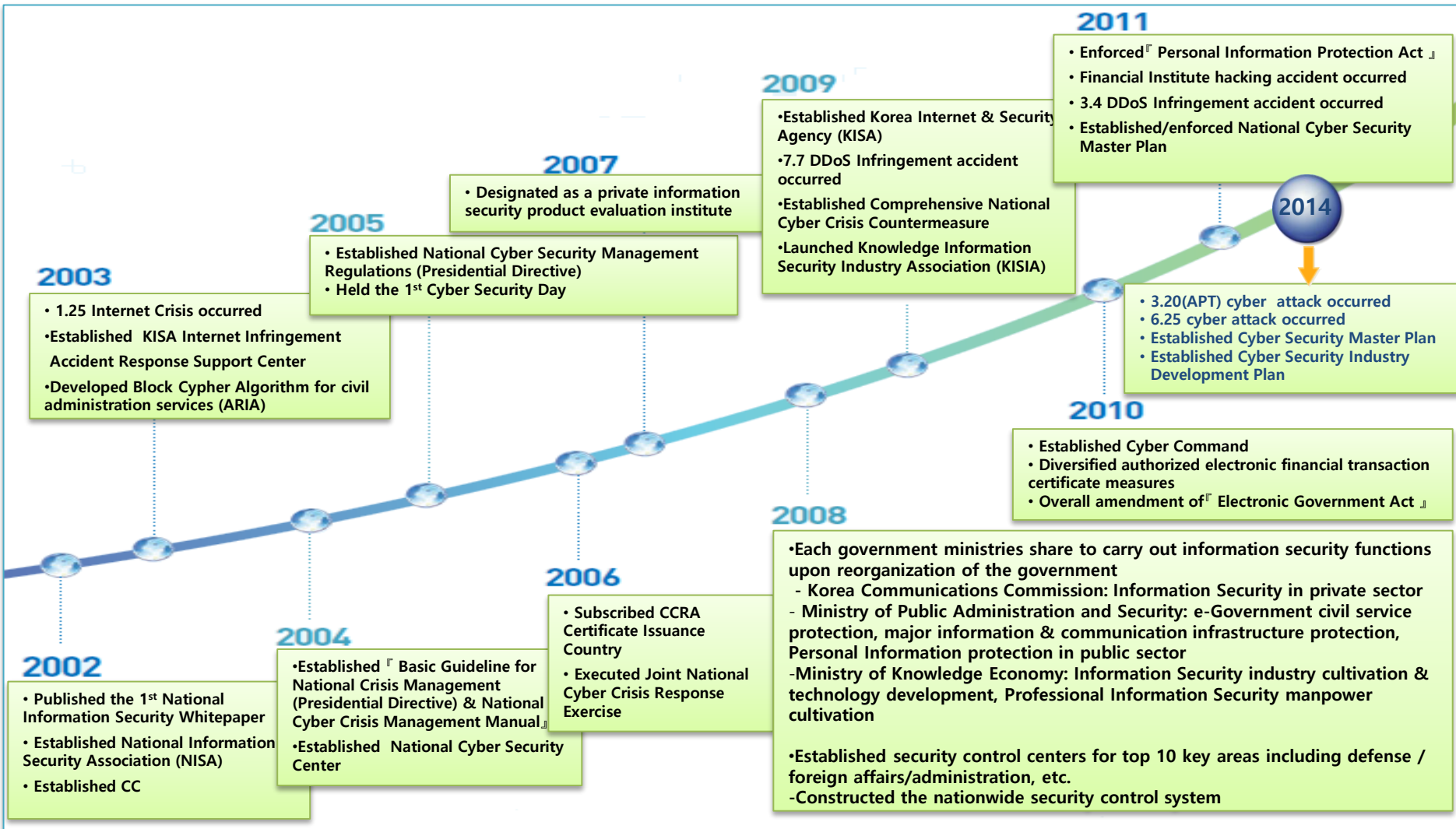
# Cyber Security Policy & Response

---

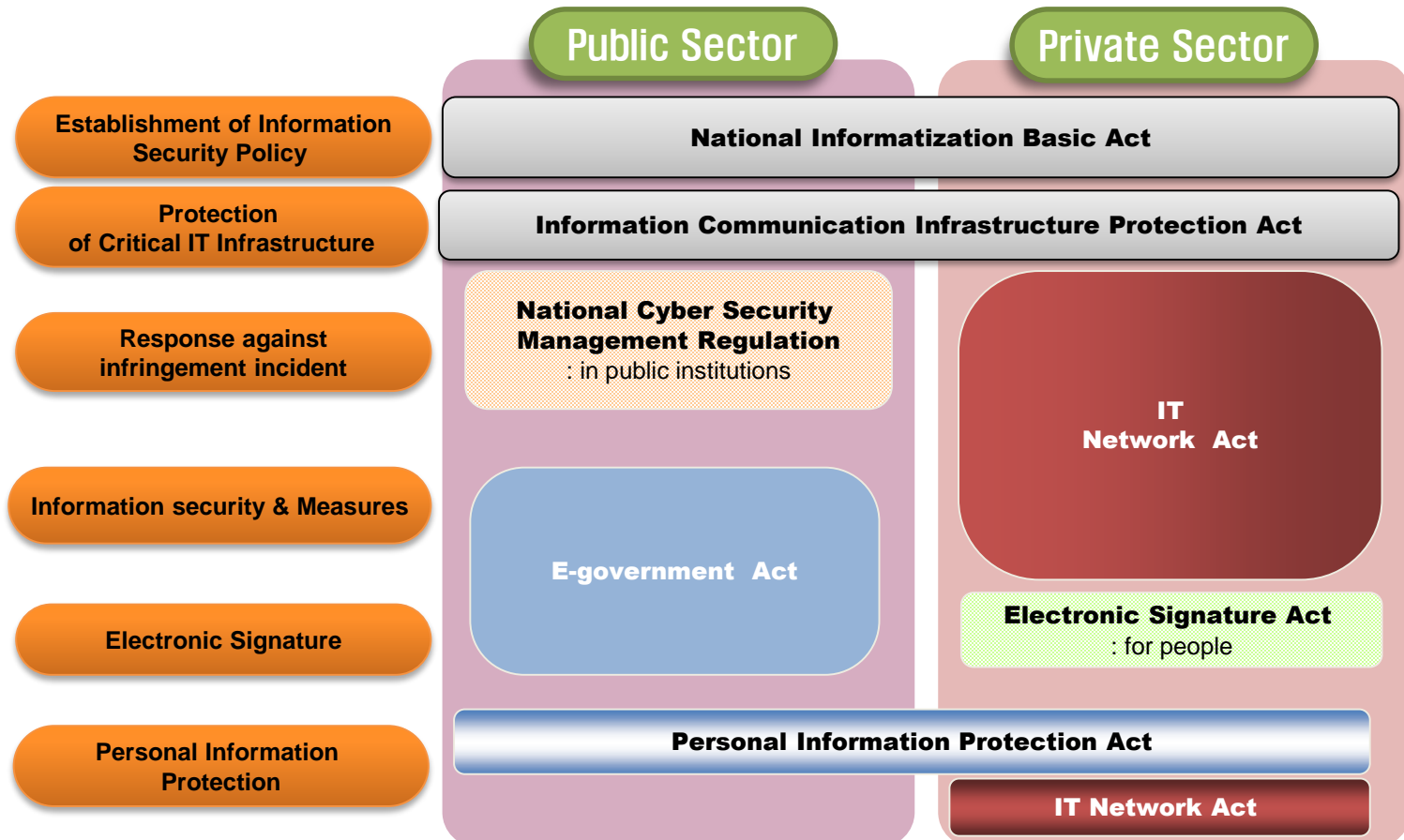
# History of Korea's Information Security Policies(1/2)



# History of Korea's Information Security Policies(2/2)

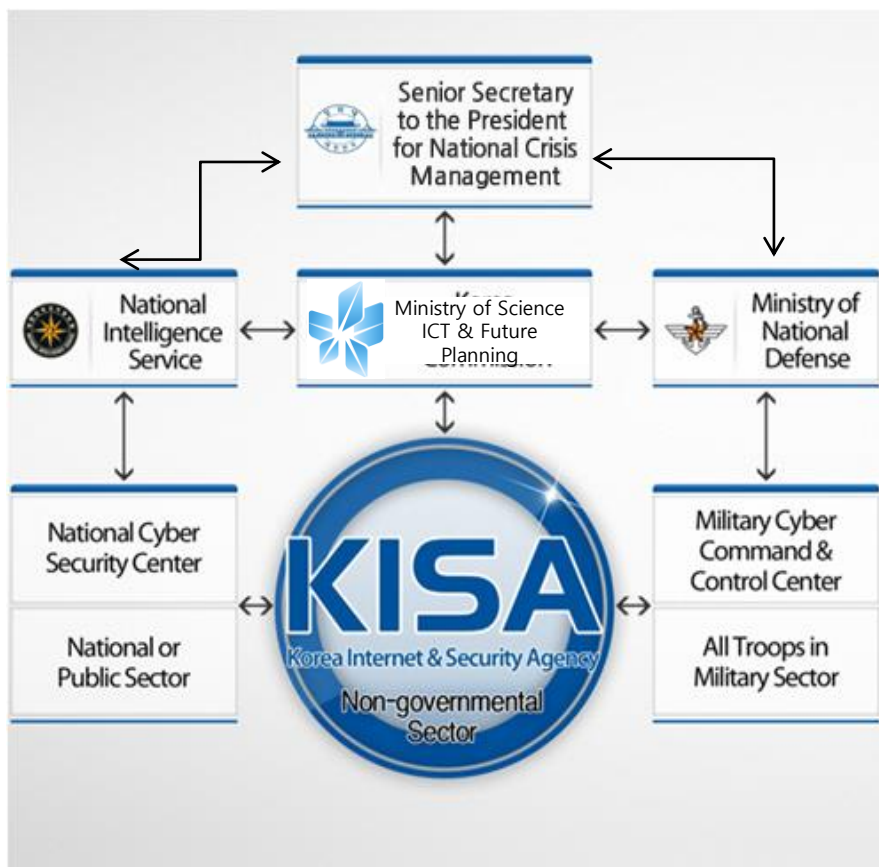


# The structure of Cyber Security law in Korea



※ IT Network Act(= Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.)

# National Cyber Security Framework



	Warning Level	Criteria for warning	Measure
<b>Critical</b>	▶ <b>Issue critical warning</b> ▶ Subject : MSIP ▶ Prior consultation with National crisis management office	• Internet communications paralysis	• Organize crisis center • Private-Public Joint investigation group • Block specific service ※ Overall response
<b>Severe</b>	▶ <b>Issue severe</b> ▶ Subject : MSIP ▶ Prior consultation with National crisis management office	• Multiple ISP network and infrastructure failure • Massive damages	• Notify specific service control • Public promotion (Media) • Emergency work system ※ Rapid response
<b>Substantial</b>	▶ <b>Issue substantial</b> ▶ Subject : MSIP	• Local Communications disorder • Internet-related Disorder	• Assess damages and report • Emergency work system ※ Tighten security
<b>Moderate</b>	▶ <b>Issue moderate warning</b> ▶ Subject : MSIP	• Increased possibility of security incident expansion and damages	• Public promotion • Tighten monitoring • Emergency work system ※ Observe signs
<b>Normal</b>	▶ <b>Normal situation</b>	▶ <b>Common response by level</b> • Consult on information (NIS, MND) and report to BH National crisis situation center • Analyze cause, prevent damage expansion and support recovery	

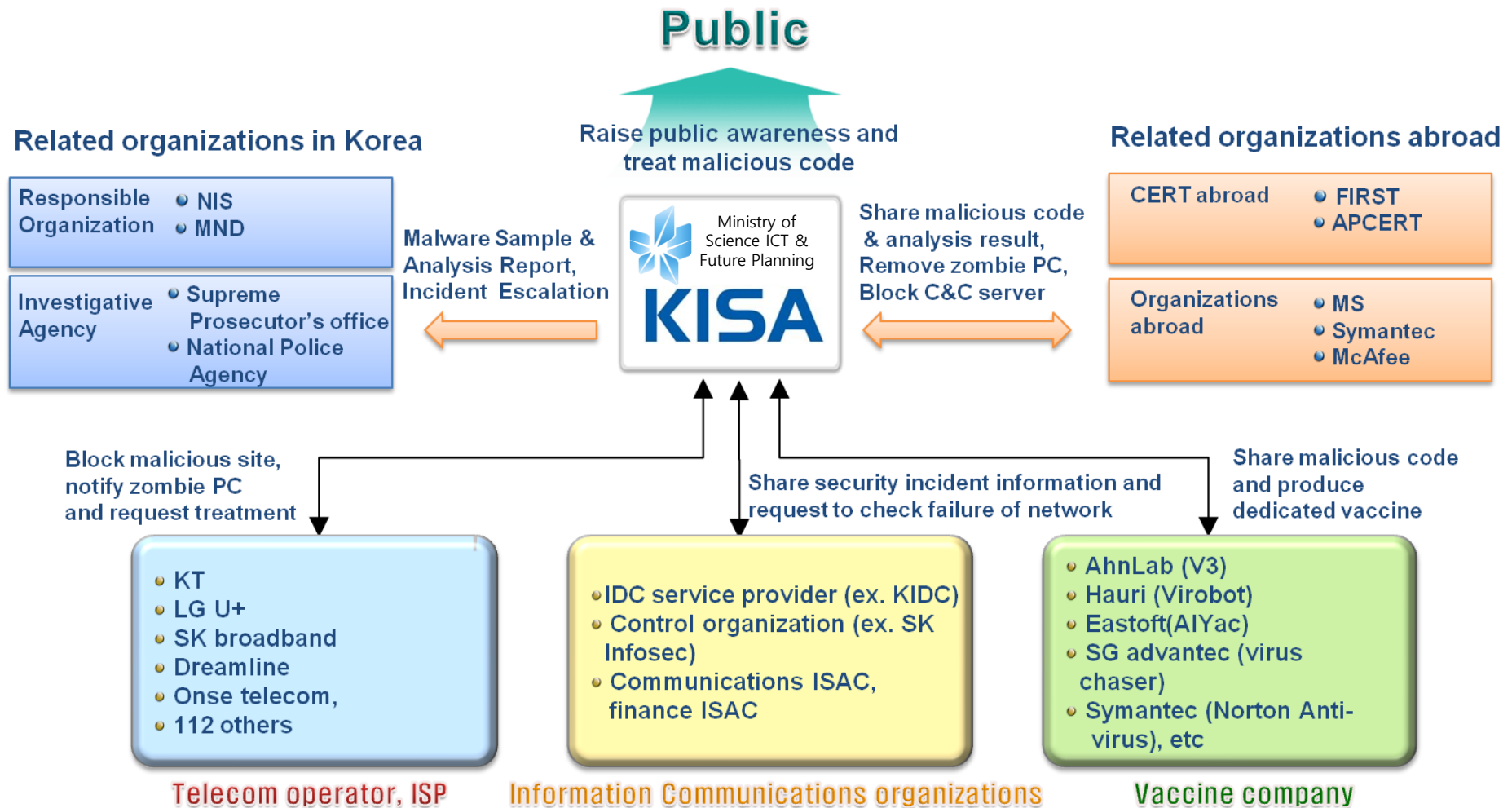
## KISA under MSIP in charge of Cyber Security of Private sector

✓ Most security incidents including zombie PC occur in private sector and KISA is responsible for that incidents

## Cyber Threat Warning System (Normal, Moderate, Substantial, Severe, Critical)

✓ MSIP/KISA is in charge of issuing cyber security alarm(Composed of 5 threat levels) for the private sector

# Cyber Threat Response Cooperation System



# KISC(KrCERT/CC) Mission and Organization

## Mission

- 7days/24hours Monitoring, Early Detection/Response on Cyber Attacks in Private sector
- Rapid Response for Nation-wide Major Internet Incidents to Prevent and Minimize damages
- Cooperation with Domestic(ISPs, Anti Virus Companies), and Foreign Partners (FIRST, APCERT, Microsoft, Symantec, etc)

## Organization

### Korea Internet Security Center

#### Internet Incident Response Division

Internet Incidents Response Planning Team

Internet Security Response Team

Internet Security Response Team

Internet Incident Detection Team

Cyber Fraud Response Team

#### Internet Incidents Analysis Division

Internet Incidents Analysis Planning Team

Internet Incident Investigation Team

Code Analysis Team

Vulnerability Analysis Team

#### Infrastructure Protection Division

Critical Infrastructure Protection & Planning Team

e-Government Security Team

IT Security Evaluation Team

Information Security Management Team

# Security Monitoring Room

- Security Monitoring Detail
  - Traffic : 158 Domestic ISP/IDC/MSO/MSSP Traffic, Ports, Protocols, Attacks
  - Web Servers : 600+ Major Domestic Web servers
  - DNS : 13 Root DNS, 6 KR DNS, 12 Major Domestic ISP DNS
  - Security Information : Major Anti-Virus, System/Software/Security Company sites
  - Honey-net / Honey-pot
  - Monitor web-embedded malicious code : 2.3 Mil Domestic Websites
  - Hotline (ISPs, Anti-Virus Companies, NCSC, etc)
- Incident Call Center Services
  - Call Center for Incidents Response & Private Outreach : +82-118 (free)



# Response Procedure(KISC)

## KISC's security incident response system

Monitoring/Detection

Quick analysis/Response

Recovery  
support/Recurrence  
prevention

Internet service provider



Cooperation at home  
and abroad



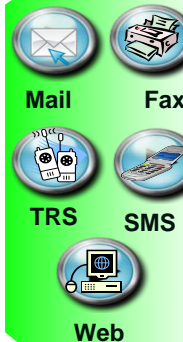
118 reporting/KISC  
detection



# KISA

Korea Internet Security Center

Traffic status  
Vulnerability information  
Malicious code information  
User report



Internet user (corporation,  
individual)



Alarm  
issuance

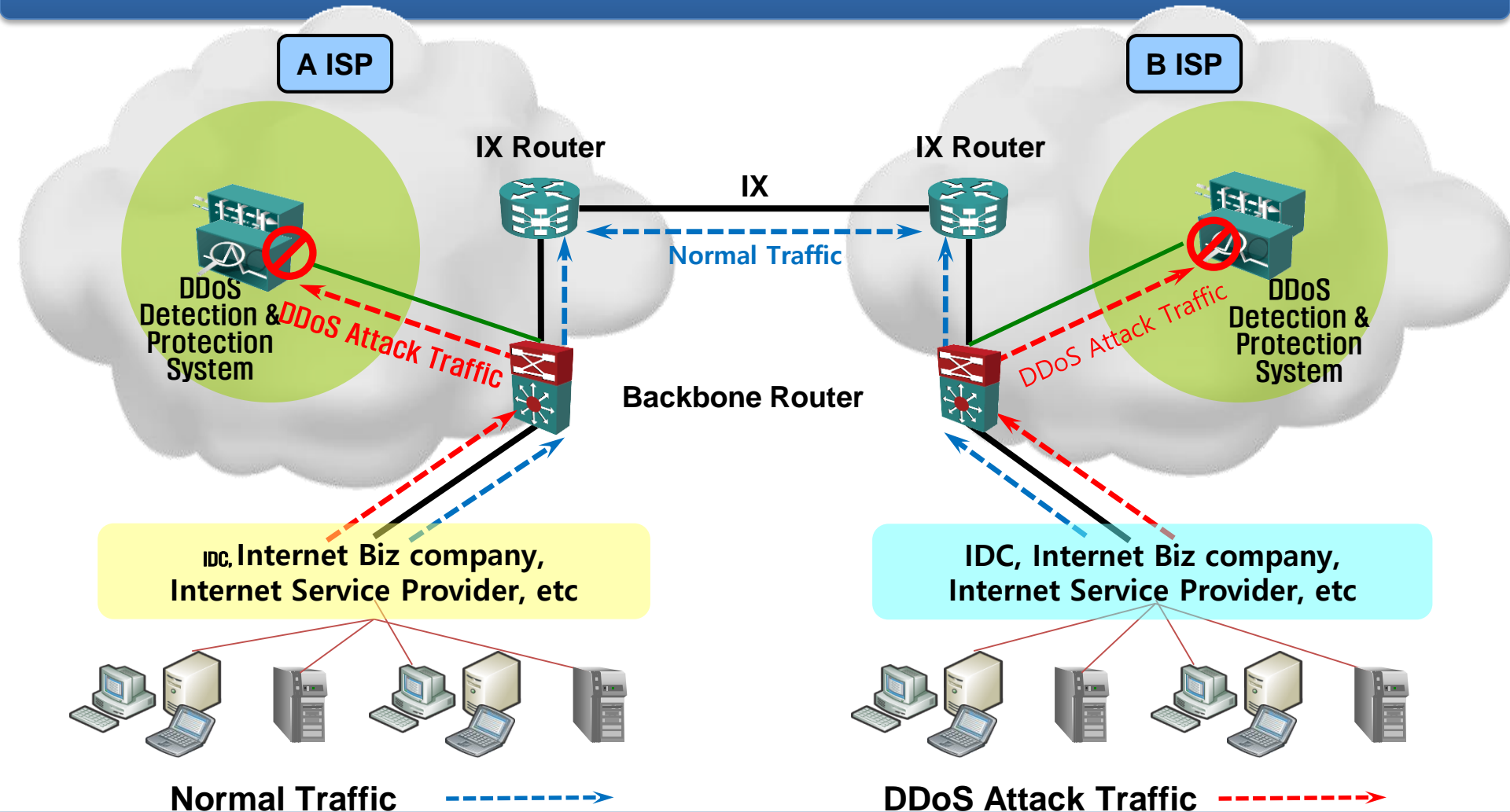
Internet service provider



# Cyber Attack Response System

## DDoS Defense System

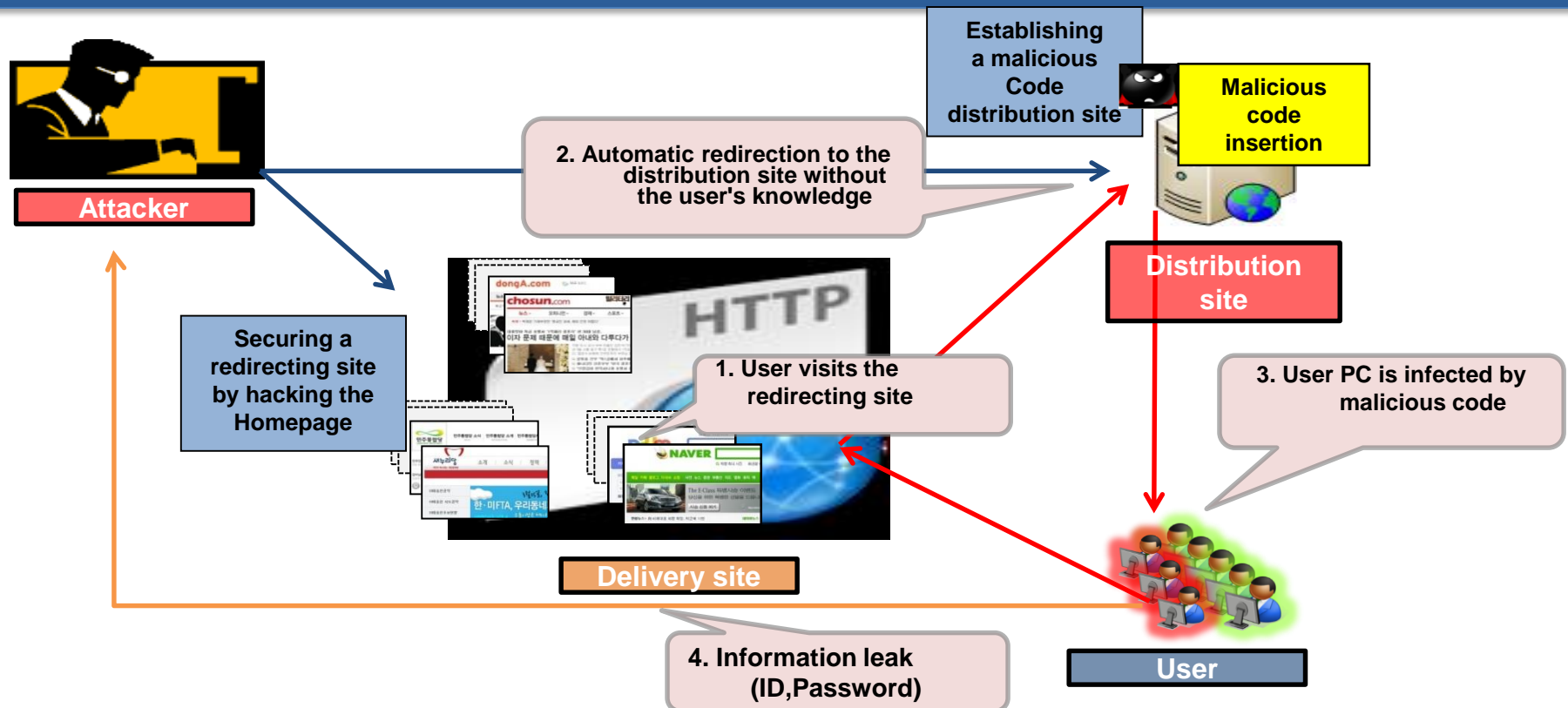
- Early DDoS attack detection at Internet Exchange (IX) node



# Cyber Attack Response System

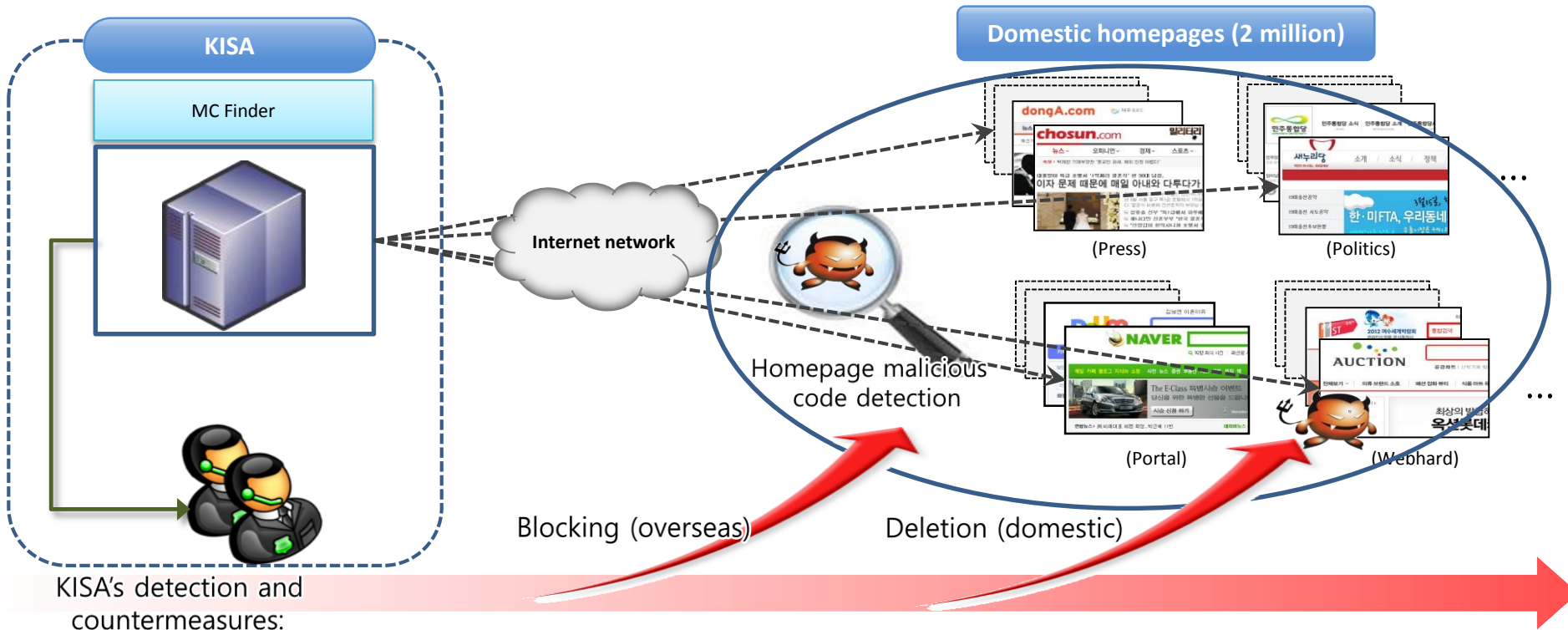
## Malicious code-hiding site detection system (MC Finder)

- Malicious code hiding-site refers to the homepage that can infect a user's PC with malicious code. The website hides malicious code itself or the URL that distributes the malicious code after upon being hacked.



# Cyber Attack Response System

## Overview diagram of detecting and handling a malicious code-hiding site



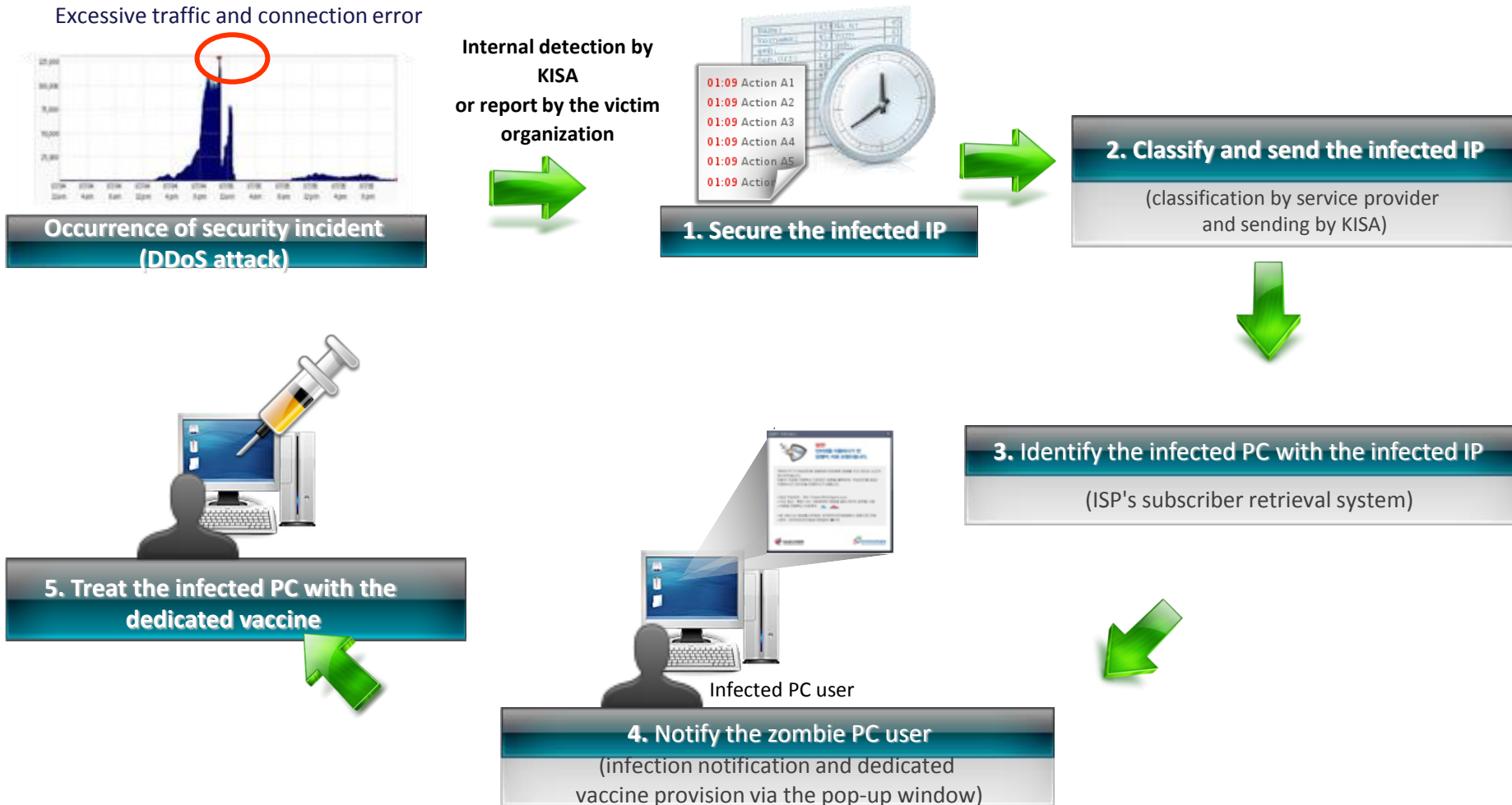
- Monitoring domestic homepages (2 million) to detect hidden malicious code (8 hours/day)

- Requesting measures to the homepage administrator via phone or official letter

- Malicious code deletion (domestic)
- Homepage blocking (overseas)

# Cyber Attack Response System

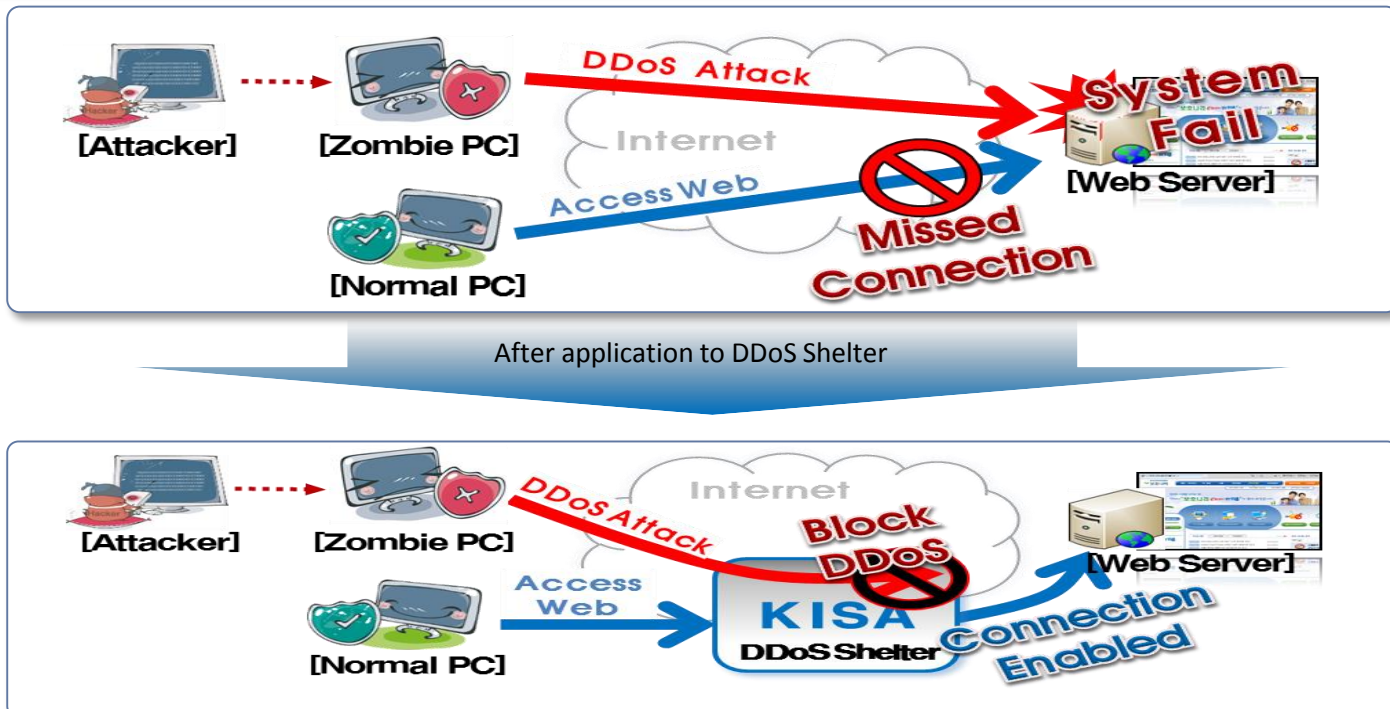
## Cyber Curing System



# Cyber Attack Response System

## Defense principle of DDoS Cyber Shelter

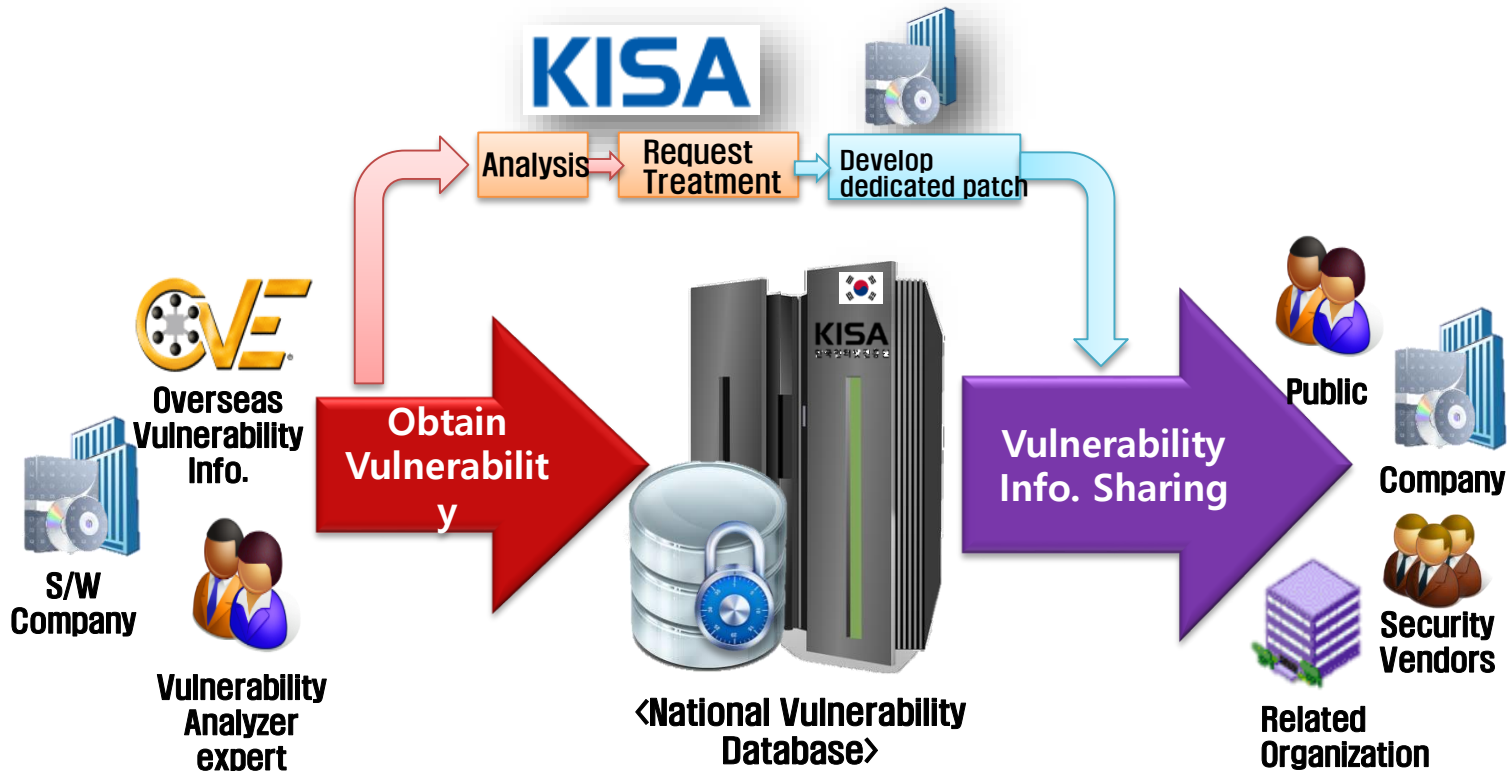
- DDoS Cyber Shelter is designed to defend effectively against two typical DDoS attack types: line bandwidth exhaustion attack and web server resource exhaustion attack.
- The line bandwidth exhaustion attack can be blocked in advance in cooperation with the line provider before shifting to Cyber Shelter.
- The web server resource exhaustion attack, which can cause serious deterioration of server availability with a small volume of traffic, can be prevented by applying the analysis result to each defense equipment through application layer traffic analysis and identification.



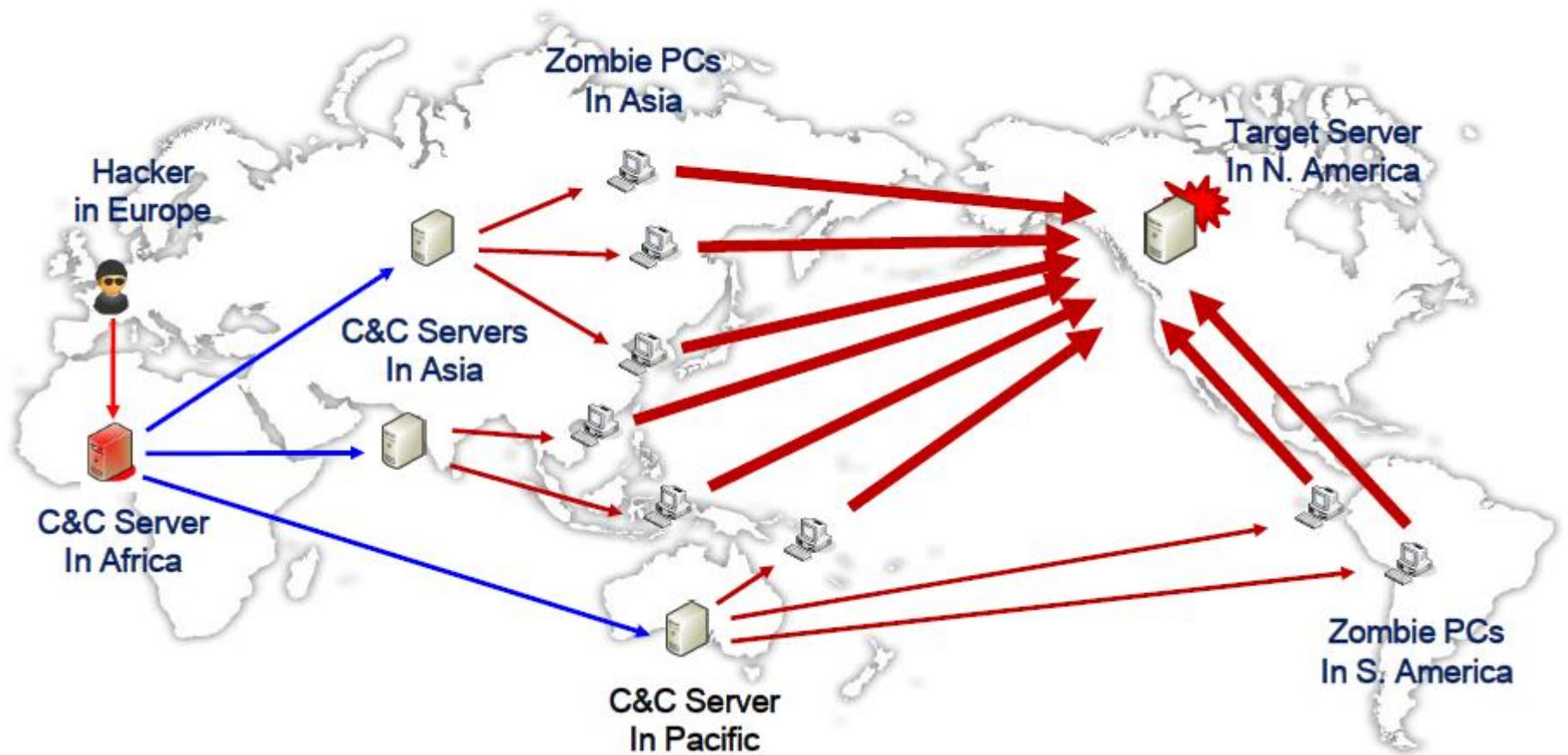
# Cyber Attack Response System

## National Vulnerability Database

- Analyze and respond using following resources : self-excavating, Vulnerability report reward program(Since Oct, 2012)
- Operate National Vulnerability Database System (Since March, 2014)



# International Cooperation to Response



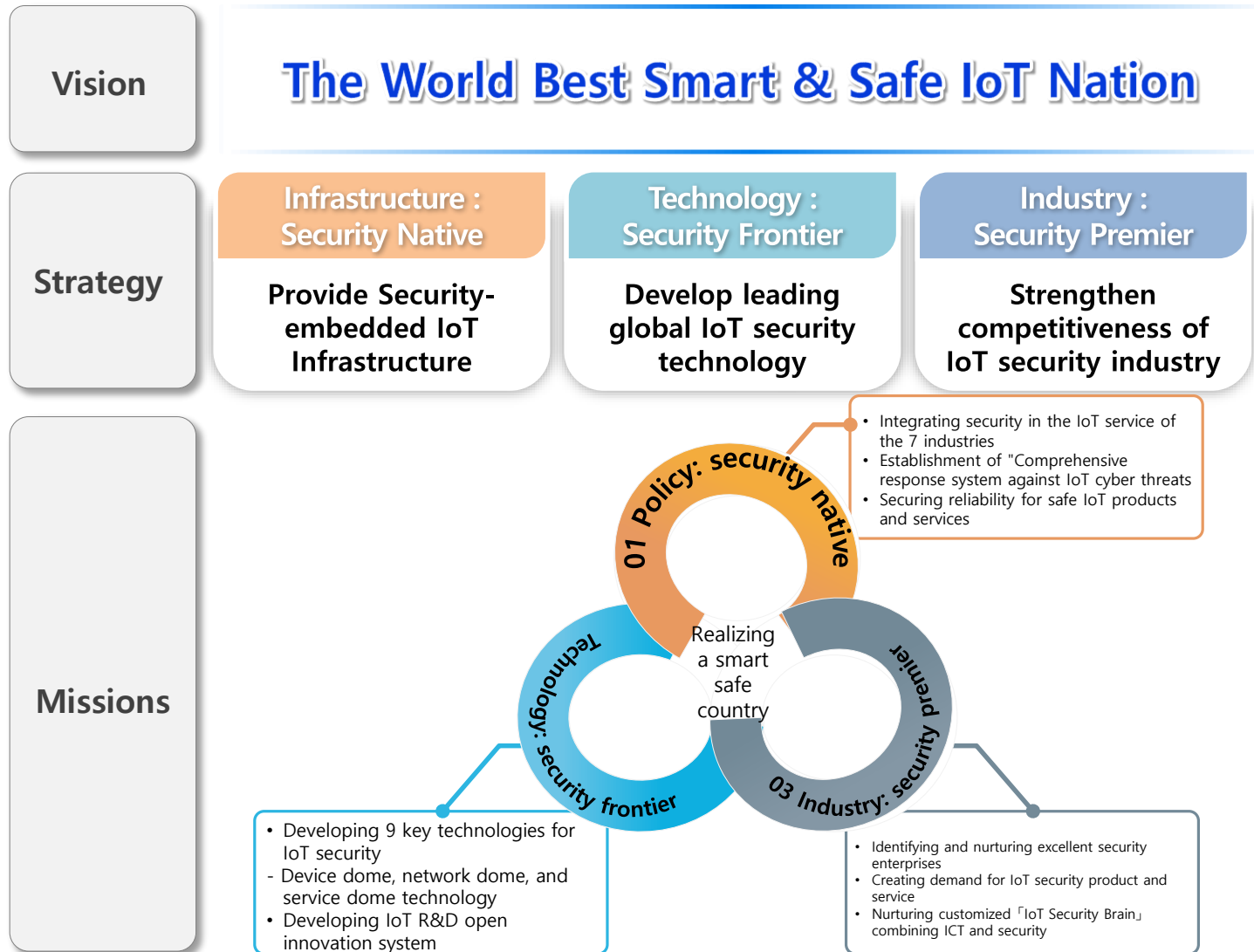


# Recent Cyber Security Strategies

---

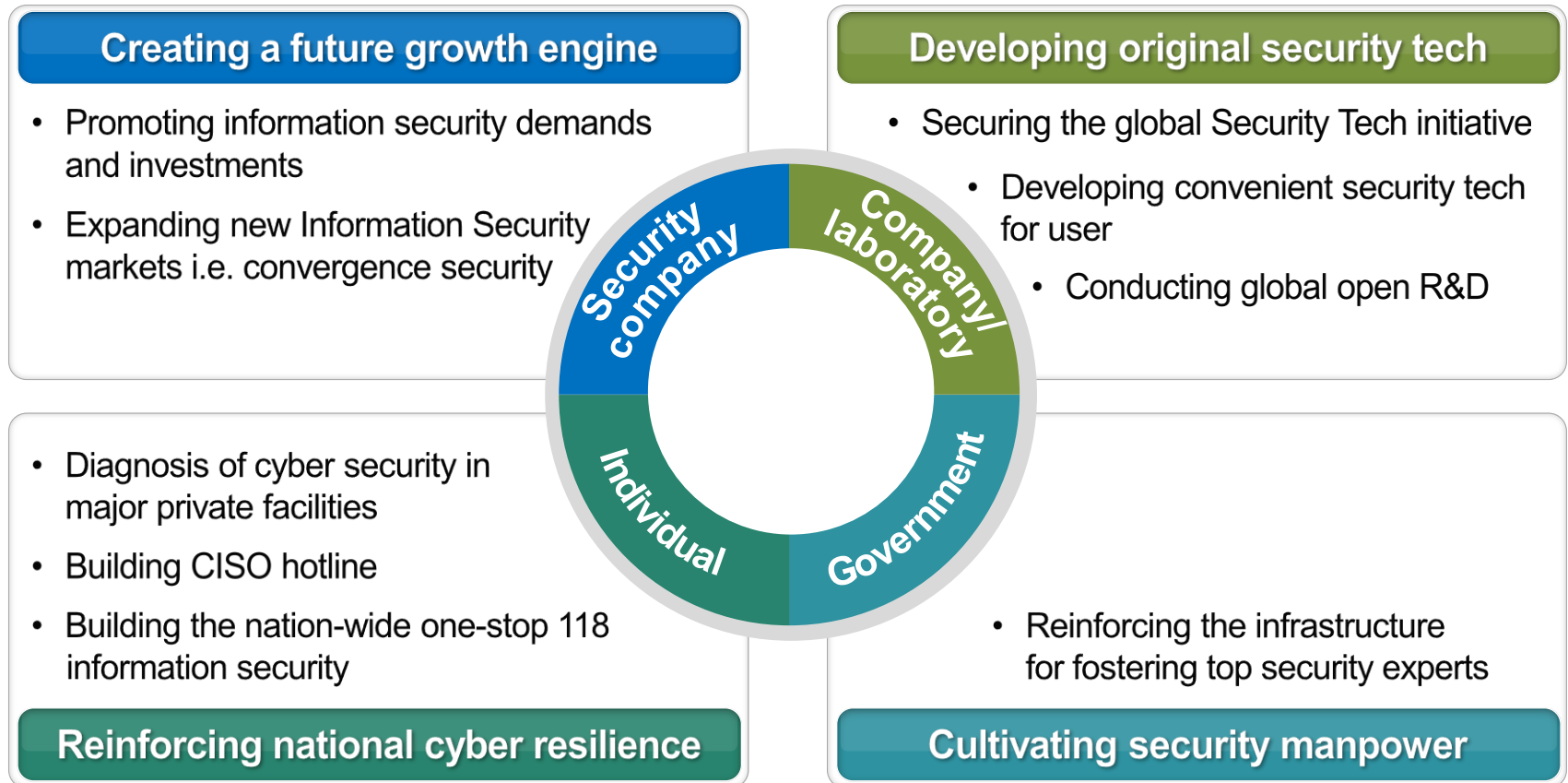
# Recent cyber security Strategies

- IoT Security Roadmap(November 2014)



# Recent cyber security Strategies

- K-ICT Security Master Plan (April 2015)



# Recent cyber security Strategies

- Cloud Security Strategy(Sept. 2015) (1/2)

Vision

Secure Cloud Country [safe K-Cloud]

Objective

**Cloud Usage Ratio**

3.3%[year 2014]



above 40%[year 2019]

Direction

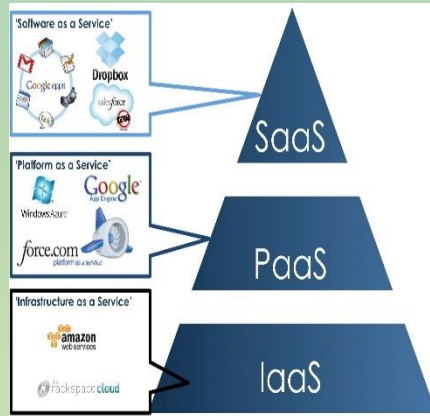
1. Reinforcing managerial & technical protective measures with the implementation of Cloud Development Act.
2. Cloud service user protection & continuous development of service protection measures
3. Maintaining the consistency with the security policy associated with the K-ICT Security Master Plan

# Recent cyber security Strategies

- Cloud Security Strategy(Sept. 2015) (2/2)

## Projects

### Improvement of info. security Lev.



**Provider**

### Establishment of security infra

Individual



Enterprise



Public  
Organization



**User**

### Promotion of info. security enterprise

Technology



Manpower



Support  
System



**I. S. Industry**

## Preemptive policy measures

Set info. security standards

Transparent info. security situation

Build incident response system

Provision of personal I. S. system

Damage prevention system

Enhancement of convenience

Secure core technology

Manpower training

Supporting Cloud security company

IV

## Global Cybersecurity Center for Development & CAMP

---

# Global Cybersecurity Center for Development

## Objective



Supporting Cyber Capacity Building for Developing Countries  
Sharing Practical Cyber Security Knowledge & Experiences

## Framework

- Positioning : A global institute in charge of enhancing cyber security capabilities for public officials
- Formation
  - Established as a virtual organization within the KISA at the moment
  - but it will transform its own characteristics toward an international institute based on close cooperation with international organizations and individual countries

## Major role



### Education

- Invitation-based Training & Joint Local Seminars
- Online Hacking Simulation Test

### Consultation

- Establishment of Cybersecurity Master Plan
- Consulting Cybersecurity Policy & Strategies
- Diagnosis of Critical Information Infrastructure Protection

### Networking

- Partnership with International Organizations
- Hosting Global Conference and forum

# Global Cybersecurity Center for Development

## Chronology



MoU between Korea  
Communications  
Commission & World  
Bank Group

Feasibility Study on  
GCCD Establishment

Legal Advisory on  
GCCD's Organizational  
Form

Establishment of  
GCCD  
in Seoul, Korea

GCCD Training  
- National Cyber  
Security Policy Course

2013.1

2014.7

2015.1

2015.6

2015.9

### Phase 1 ('15 ~ '16)

#### Establishment & operation

- '15.06.29 : Establishment of GCCD
- '15.04~08 : Development of Training curriculum and materials
- '15.09~12 : Opening up official homepage
- '15.09~12 : Invitation-based Training and Korea-WB local seminar(twice)

### Phase 2('15 ~)

#### External Partnership

- '15.08~10 : Collaborating with Oxford Cyber Security Capacity Center
- '15.10~12 : Register as an Initiative of GFCE(Global Forum on Cyber Experts)
- '16~ : Online education platform, information security consulting, expanding external partnership with domestic/international organizations

# CAMP(Cyber-security Alliance for Mutual Progress)

## Major cybersecurity threats all over the world



Cybersecurity cannot be handled by a single country or organization



Information Security is an endless marathon between shield and spear  
Global collaboration is essential to better response

# CAMP(Cyber-security Alliance for Mutual Progress)



[Area]

Spam  
Response

PKI

Personal Data  
Protection

IoT  
Security

Critical Infra.  
Protection

[Mode]

Consultation about  
the cybersecurity  
policy

Education and  
training in  
information  
security

Information  
sharing on  
cybersecurity  
framework

Sharing hands-on  
experience on  
incident response

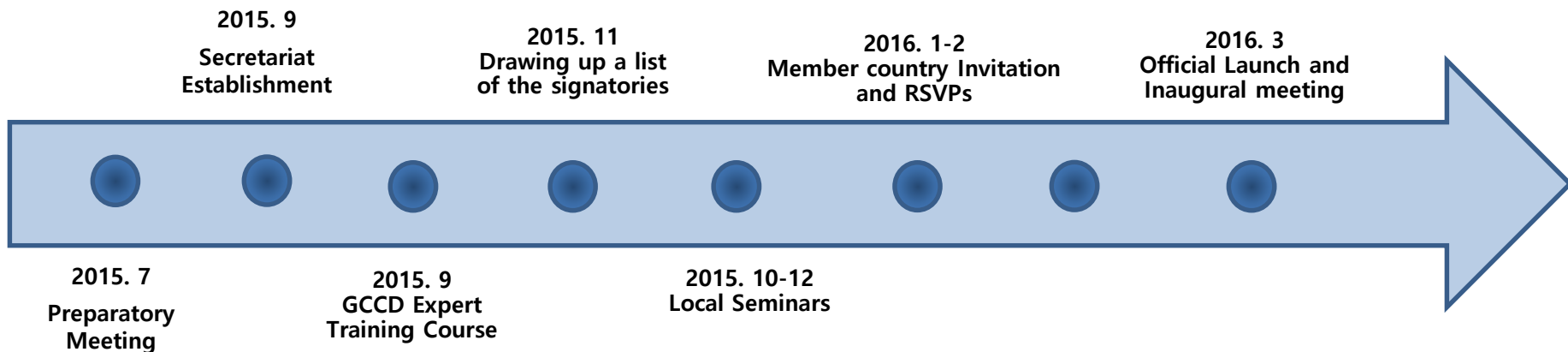
# CAMP(Cyber-security Alliance for Mutual Progress)

## Progress

### • 2015. July : CAMP Preparatory Meeting

- Participants : 60 Officials from 28 countries(Ministry, government agency, Security firms, etc.)
- Achievements : CAMP promotion plan establishment, Statement on CAMP launching

## Road Map



# Thank You